The 4th Amendment and Government Surveillance of Electronic Communications

Has Technology Outrun the Constitution?

Constitution Day Presentation

Georgia Institute of Technology

Lawrence P. Keller, Of Counsel
Sapronov & Associates, PC

September 20, 2007

Central Issue

- Whether 4th Amendment guarantees have kept pace with new technologies such as e-mail

Outline

- A brief history of the 4th Amendment
- The statutory scheme
  - Wiretap Act & Electronic Communications Privacy Act
  - Stored Communications Act
- Recent developments
- Conclusions

Two Important Distinctions

- ***Communication content*** **vs. transactional information**
- ***Government surveillance connected to domestic criminal investigations*** **vs. surveillance concerning foreign intelligence**

The Fourth Amendment to the Constitution

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issues, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

1928 *Olmstead* Case Rejected Argument that Wiretap Was Illegal – 4th Amendment Applies Only to Physical Entry

The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.

Brandeis Dissent Foresaw Increased Government Invasion of Privacy with Development of New Technologies

The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

1967 *Katz* Decision Overturned *Olmstead* - Reasonable Expectation of Privacy was Key, Not Physical Entry

Once it is recognized that the Fourth Amendment protects people - and not simply "areas" - against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.

Wiretap Act of 1968 Required Court Order Based On Probable Cause

- Before *intercepting* a conversation by wiretap or eavesdropping device, law enforcement must obtain court order based on showing that (i) there is probable cause to believe that a crime has been or is being committed, (ii) the conversations to be intercepted must be particularly described, (iii) the surveillance must be for a specific, limited period of time.

Wiretap Act of 1968 Required Court Order Based On Probable Cause

- For purposes of a wiretap, probable cause is a showing of facts sufficient to support belief that
  - a particular offense is being committed; and
  - particular communications concerning that offense will be obtained through interception.

- Requirement applied only to
  - "Wire communications" – communications by telephone or telegraph
  - "Oral communications" – speech uttered by a person having an expectation of privacy

Electronic Communications Privacy Act of 1986 Extended Wiretap Act Protection to Other Forms of Communication

- "Electronic communications" – any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted by a wire, radio, electromagnetic, photo-electronic or photo-optical system
- "Interception" - intentional "acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device"
  - Communication must be in "transit" – i.e., "acquisition of communications must be contemporaneous with transmission" – otherwise it is in "storage"

Stored Communications Presents Special Problems In Applying 4th Amendment Protections

- Stored electronic communications (e.g., e-mail) generally reside on the servers of a third party Internet service provider ("ISP"); thus, issue whether user has a "reasonable expectation of privacy"
- As a private party, ISP is not subject to 4th Amendment requirements – can voluntarily turn over e-mail to government

Stored Communications Act of 1986 Affords Some Privacy Protection

- ISP serving the public cannot *voluntarily* disclose contents of stored communications to law enforcement agency unless communications
  - (i) were inadvertently obtained by the service provider; and
  - (ii) appear to pertain to the commission of a crime

Stored Communications Act of 1986 Affords Some Privacy Protection

- **Government can compel disclosure by ISP *serving the public***
  - **for e-mail that are in "temporary" storage (180 days or less) *only* by a *search warrant* (issued under the *probable cause* standard)**
  - **for e-mail in more permanent storage (greater than 180 days) either by *search warrant, subpoena* or by *court order* supported by *reasonable grounds* (a standard less than probable cause)**
  - **Opened vs. unopened e-mail**
    - **Above rules apply to non-public providers only if the email is unopened**

Summary So Far

- Under ECPA, electronic communications in transit are afforded full 4th Amendment protection (i.e., can be intercepted based only on a *search warrant* showing probable cause*)*
- Stored electronic communications is afforded some, but not complete, 4th Amendment-type protection under the SCA
- Users of non-public network services provided to an affiliated group (e.g., a university's or business's e-mail system) are afforded less protection under the SCA than users of an ISP serving the public

Questions

- If the critical 4th Amendment objective (as per *Katz*) is to protect an individual's reasonable expectation of privacy, why should it matter if electronic communications is in transit or storage with an ISP?
- Why should it matter if the ISP is offering service to the public or not?

Warshak v. US – Is Constitution Finally Catching Up with Technology?

- Facts
  - Subpoena's issued to ISPs under SCA to compel disclosure of content of defendant's stored (over 180 days) e-mails
    - Supported by standard of "reasonableness" which requires less of a showing than probable cause
  - Defendant filed suit arguing that the compelled disclosure of his e-mails by the ISPs without a warrant supported by probable cause violated the Fourth Amendment

Warshak v. US – Is Constitution Finally Catching Up with Technology?

- U.S. Court of Appeals, 6th Circuit reasoned
  - Even if e-mails are stored by a third-party ISP, user could have a "reasonable expectation of privacy" if ISP would not ordinarily view content of e-mails
    - Court distinguished between situations where
      - agreement between user and ISP allowed ISP to continually monitor and audit content of e-mails – in which case there would be no expectation of privacy, and
      - agreement between user and ISP did not allow ISP access to content of emails at all, or allowed access only under extraordinary circumstances – in which case there would be an expectation of privacy

Warshak v. US – Is Constitution Finally Catching Up with Technology?

- U.S. Court of Appeals, 6th Circuit ruled
  - Under the facts of this case, defendant had a reasonable expectation of privacy
  - Government was not allowed to compel disclosure of contend of defendant's emails without a warrant supported by probable cause

Conclusions

- ***Warshak*** **case is the first court decision making "expectation of privacy" – as it should be - the determining factor in deciding whether a warrant supported by probable cause is required for e-mails stored by ISPs**
  - **Remarkably, this comes 40 years after *Katz* and 21 years after start of ECPA/SCA statutory regime**
  - **Only applies in the 6th Cir., not clear if other courts will follow, or whether Supreme Court will review**

Conclusions

- Presumably, *Warshak* would apply to private network service providers such as university e-mail systems
  - But private providers are more likely to subject e-mails to regular monitoring as part of terms of use
- Should Congress amend SCA consistent with *Warshak?*